

(To be used in proposal process documents)

**§2.9 COMPLIANCE WITH FEDERAL HIPAA AND STATE CONFIDENTIALITY LAW**

- A. The Contractor acknowledges its duty to become familiar with and comply, to the extent applicable, with all requirements of the federal Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1320d et seq. and implementing regulations including 45 CFR Parts 160 and 164. The contractor also agrees to comply with the Maryland Confidentiality of Medical Records Act (Md. Code Ann. Health-General §§4-301 et seq., MCMRA). This obligation includes:
  - 1. As necessary, adhering to the privacy and security requirements for protected health information and medical records under federal HIPAA and State MCMRA and making the transmission of all electronic information compatible with the federal HIPAA requirements; and
  - 2. Otherwise providing good information management practices regarding all health information and medical records.
- B. If the Department determines that functions to be performed in accordance with the Services to Be Performed set forth in Part I constitute business associate functions as defined in HIPAA, the selected offeror must execute a business associate agreement as required by HIPAA regulations at 45 CFR §164.501 and set forth in Appendix \_\_\_\_\_. The fully executed business associate agreement must be submitted within 10 working days after notification of selection, or within 10 days after award, whichever is earlier. Upon expiration of the ten-day submission period, if the Department determines that the selected offeror has not provided the HIPAA agreement required by this solicitation, the Procurement Officer, upon review of the Office of the Attorney General and approval of the Secretary, may withdraw the recommendation for award and make the award to the next qualified offeror.
- C. Protected Health Information as defined in the HIPAA regulations at 45 CFR 160.103 and 164.501, means information transmitted as defined in the regulations, that is individually identifiable; that is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and that is related to the past, present, or future physical or mental health or condition of an individual, to the provision of healthcare to an individual, or to the past, present, or future payment for the provision of healthcare to an individual. The definition excludes certain education records as well as employment records held by a covered entity in its role as employer.